Template for use by
the U.S. Federal PKI Policy Authority for Cross-Certifying with
U.S. Federal Agencies and other U.S. Federal Entities, with
U.S. State and Local Governments and U.S. Private Sector Entities, and with
Governments of other Nations
(Note: The cross-certifying Entity may substitute its name for the word "Entity" as appropriate.)
(Note: This and any other italicized text in the template will be deleted when making an actual MOA.)

Memorandum of Agreement

I. Introduction

A. The Parties. This Agreement is entered into by the United States Federal Public Key Infrastructure (PKI) Policy Authority ("Federal PKI Policy Authority") and _____ ("Entity").

B. The Agreement. This Memorandum of Agreement ("MOA") details the agreement between the Entity and the Federal PKI Policy Authority covering interoperability between the Entity Principal Certification Authority (CA) and the Federal Bridge Certification Authority (FBCA). Specifically, it sets forth the rights, responsibilities and reservations of both Parties governing Entity's interoperation with the FBCA.

C. The Entity Principal CA. The Entity Principal CA to which this MOA pertains is _____.

D. The Points of Contact. The Points of Contact for notifications and other communications between the Parties shall be the individuals identified at the end of this MOA, except as may be specified in this MOA or such other persons agreed upon by the Parties separately from this MOA but documented in official correspondence between the Parties.

II. Background

A. The FBCA is designed to provide a mechanism for agencies (and other entities) of the US Federal Government that employ entity-specific PKI domains to interoperate efficiently. The FBCA facilitates the ability of entities to create and process trust paths between entity-specific PKI domains, so that digital certificates issued by CAs in one domain can be honored with an appropriate level of trust in a different domain.

B. The FBCA acts as a non-hierarchical "hub." An entity Principal CA receives permission to interoperate with the FBCA under terms and conditions described in this document. This system allows every CA that interoperates with the FBCA the possibility of interoperating with all participating entities using the FBCA-issued certificates, in an

environment of trust and reliability. This is accomplished through the use of policy mapping, which is how certificates issued in different entity PKIs meet one another's standards for authentication, integrity of data, non-repudiation, and encryption of data. A policy mapping of an entity Principal CA level of assurance in terms of an FBCA CP level of assurance is approved by the Federal PKI Policy Authority, and then placed in the certificate issued by the FBCA to the entity Principal CA. In some cases the entity CP does not include all the policy detail necessary for that mapping, and the supplemental requirements are provided from other sources such as the corresponding entity CPS and laws, regulations or data center policies that apply to the operation. These Supplemental Requirements, if any, are catalogued in Appendix A of this MOA to explain how each relates to the policy mapping.

C. Similarly, a policy mapping of an FBCA level of assurance in terms of an entity Principal CA level of assurance is approved by the entity, and then placed in the certificate issued by the entity Principal CA to the FBCA.

D. When the Entity is determining whether to rely on a certificate issued by another entity or party, however, it is not required to use the mapping expressed in the FBCA certificates. The Entity, at its sole discretion, may choose to use a separate mapping for certain transactions or for all transactions, and may express such a mapping in the certificate it issues to the FBCA. Entities must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each entity for each application and is not controlled by the FBCA. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

III. Scope

A. This Agreement is binding only upon the Parties, by and through their officials, agents, employees, and successors. No person or entity is intended to be a third party beneficiary of the provisions of this Agreement for purposes of any civil, criminal, or administrative action, and accordingly, no third person or entity may assert any claim or right as a beneficiary or protected class under this Agreement in any civil, criminal, or administrative action. Similarly, this Agreement does not authorize, nor shall it be construed to authorize, access to any documents by persons or entities not a Party to this Agreement, except entities that are cross-certified with the FBCA.

B. The Entity's Application for Interoperability with the Federal Bridge Certification Authority ("Application") is incorporated into this document by reference. That Application includes both the Certificate Policy (CP) and Certification Practices Statement (CPS) that pertain to the Entity's Principal CA. The latter two documents in their current form as of the effective date of this MOA are also incorporated into this MOA by reference. The Entity Principal CA CP version is _____. The Entity Principal CA CPS version is _____.

C. The FBCA Certificate Policy is incorporated into this document by reference. The version is _____.

D. This Agreement shall constitute the entire integrated Agreement of the Parties. No prior or contemporaneous communications, oral or written, or prior drafts shall be relevant or admissible for purposes of determining the meaning of any provisions herein in any litigation or any other proceeding.

E. If, at any time, either Party to this Agreement desires to modify it for any reason, that Party shall notify the other Party in writing of the proposed modification and the reasons for it. No modification shall occur unless there is written acceptance by both Parties.

IV. Rights and Obligations of the Parties

This section details the rights and responsibilities of the Parties. It describes what the Federal PKI Policy Authority and the Entity will provide to each other and what each agrees to do in return.

A. Rights of the Federal PKI Policy Authority.

1. By entering into this agreement, the Entity grants the Federal PKI Policy Authority the rights set forth in the FBCA CP, including appropriate access to Entity information such as CA audit results and operational information.

2. If at any time the Federal PKI Policy Authority determines that the Entity is not operating at the Level of Assurance specified in this MOA, the Policy Authority shall notify the Entity and may unilaterally reduce the Level of Assurance expressed in the certificate issued to the Entity or may revoke the certificate. The Policy Authority shall provide the Entity an opportunity to cure the assurance issues and regain its original Level of Assurance.

B. Rights of the Entity. By entering into this agreement, the Federal PKI Policy Authority grants to the Entity these rights.

1. The Entity, when relying on an FBCA certificate issued to a third party, may at its sole discretion choose to use a policy mapping different from that expressed in the FBCA certificate.

2. The Entity, when issuing a certificate to the FBCA, may express a policy mapping different from that expressed in the other certificate in the cross-certificate pair.

3. The Entity has the rights corresponding to the responsibilities of the Federal PKI Policy Authority and Operational Authority as set forth in this MOA.

4. If at any time the Entity determines that the FBCA is not operating at the Level of Assurance specified in this MOA, the Entity shall notify the Federal PKI Policy Authority and may unilaterally reduce the Level of Assurance expressed in

the certificate issued to the FBCA or may revoke the certificate. The Entity shall provide the FBCA an opportunity to cure the assurance issues and regain its original Level of Assurance.

C. Responsibilities of the Federal PKI Policy Authority. By entering into this agreement, the Federal PKI Policy Authority agrees that it will do the following:

1. Oversee and ensure, through the FBCA Operational Authority, proper performance of the operation and maintenance of the FBCA and the FBCA Directory in accordance with the FBCA CP and CPS. Among other things, this includes the following:

a. Identity Proofing. For certificate Subjects, the FBCA shall ensure that the applicant's identity information is verified and checked in accordance with the applicable CP and CPS.

b. Private Key Protection. The FBCA shall protect the private key corresponding to the cross-certificate issued by the Entity, as required for the level of assurance at which the FBCA operates.

2. Maintain compliance with the requirements of this MOA, or promptly notify the Entity in the event of an actual or expected nonconformance.

3. Make its compliance audit reports available to the Entity.

4. Respond within a reasonable time to any requests for information by the Entity.

5. Issue a cross certificate to the Entity Principal CA, indicating its policy mapping as determined by the Federal PKI Policy Authority, and including name constraints appropriate for the Entity PKI.

6. Make the certificates and certificate status information in the FBCA directory publicly available through the Internet.

7. Promptly advise the Entity (1) in the event of any material problem or inability to operate the FBCA in accordance with the FBCA CP or CPS, or (2) in the event that the Federal PKI Policy Authority becomes aware of a material non-compliance on the part of any other party that is within the name constraints in the cross-certificate issued by the FBCA and that interoperates with the FBCA or (3) in the event that the FBCA takes any action to terminate or limit such other party's interoperability with the FBCA. Any such notification will occur as follows:

a. The FBCA Program Manager, or the Chair of the Federal PKI Policy Authority, shall notify the Entity points of contact.

b. Notification will be done by telephone, by digitally signed e-mail, or by any other mechanism agreed upon by the Parties separately from this agreement but documented in official correspondence between the Parties, signed by the Chair of the Federal PKI Policy Authority and _____ at the Entity.

c. The FBCA Operational Authority or the Federal PKI Policy Authority shall notify the Entity at the earliest feasible time in the event of an FBCA private key compromise or loss or another cross-certified entity's Principal CA private key compromise or loss. A CARL shall be published at the earliest feasible time by the FBCA Operational Authority.

d. The FBCA shall at the earliest feasible time securely advise the Federal PKI Policy Authority and all of its cross-certified entities in the event of a disaster where the FBCA or an entity Principal CA installation is physically damaged and all copies of the FBCA or entity Principal CA signature keys are destroyed.

8. Review the FBCA CP and CPS at least once a year for changes that become necessary from time to time. When the FBCA CP is changed, the cross-certified entities will automatically be kept notified through their participation in the routine operations of the Federal PKI Policy Authority. The Federal PKI Policy Authority shall post the revised FBCA CP on its web site.

D. Responsibilities of the Entity. By entering into this agreement, the Entity agrees that it will do the following:

1. Comply with the applicable requirements of the FBCA CP, its own CP and CPS and such other requirements (e.g., laws, regulations, data center requirements) as govern the operation of the Entity PKI. Among other things, this includes the following:

a. Identity Proofing. For certificate Subjects, the Entity shall ensure that the applicant's identity information is verified and checked in accordance with the applicable CP and CPS.

b. Private Key Protection. The Entity shall protect the private key corresponding to the cross-certificate issued by the FBCA, as required for the level of assurance at which the Principal CA operates.

2. Maintain compliance with the requirements of this MOA, or promptly notifying the Federal PKI Policy Authority in the event of an actual or expected nonconformance.

3. Ensure that third party compliance audits are performed and the results promptly reported to the Federal PKI Policy Authority as required in the FBCA CP. When multiple compliance audits are performed, the Entity may provide summaries of audits once per year.

4. Respond within a reasonable time to any requests for information by the Federal PKI Policy Authority or the FBCA Operational Authority.

5. Issue a cross certificate to the FBCA, indicating its policy mapping as determined by the Entity.

6. Make publicly available through the Internet a repository containing the certificates, certificate status information and any other information necessary to support interoperation of the Entity PKI domains that employ the FBCA for this purpose.

7. Promptly advise the FBCA Operational Authority and the Federal PKI Policy Authority (1) in the event of any material problem or inability to operate the Principal CA in accordance with the Entity Principal CA CP or Supplemental Requirements, or (2) in the event that the Entity becomes aware of a material non-compliance on the part of any other party that is within the name constraints in the cross-certificate issued by the FBCA and that interoperates with the Principal CA or (3) in the event that the Entity takes any action to terminate or limit such other party's interoperability with the FBCA. Any such notification will occur as follows:

a. The Entity shall notify the FBCA Operational Authority and the Chair of the Federal PKI Policy Authority.

b. Notification will be done by telephone, by digitally signed e-mail, or by any other mechanism agreed upon by the Parties separately from this agreement but documented in official correspondence between the Parties, signed by the Chair of the Federal PKI Policy Authority and _____ at the Entity.

c. The Entity shall notify the FBCA Operational Authority and the Federal PKI Policy Authority at the earliest feasible time in the event of an Entity Principal CA private key compromise or loss. A CARL shall be published at the earliest feasible time by the Entity CA.

d. The Entity shall at the earliest feasible time securely advise the FBCA Operational Authority and the Federal PKI Policy Authority in the event of a disaster where the Entity Principal CA installation is physically damaged and all copies of the Entity Principal CA signature keys are destroyed.

8. Review the FBCA CP when it is changed, and review the Entity CP and CPS for changes that become necessary from time to time.

9. Promptly notify the Federal PKI Policy Authority in the event of any change to the information in its Application, if possible before the change takes effect. This includes any change in the Entity Principal CA CP and changes in the provisions of the corresponding CPS (or other Supplemental Requirements) upon which the Federal PKI Policy Authority relied when mapping the Entity CP to the FBCA's certificate levels of assurance. The notification shall include the former and new versions where the change occurs, and the effective date of the change.

10. Ensure that the use of "critical" extensions is interoperable with the FBCA. If the use of such "critical" extensions should render interoperability with the FBCA inoperable, use of the "critical" extensions will be stopped immediately and all certificates issued with said "critical" extension will be revoked to stop the further disruption of FBCA operational capabilities.

11. In the case where one Entity CA certifies another CA within that Entity, the certifying CA must impose restrictions on the name space authorized in the certified CA which are at least as restrictive as its own name space.

12. Also, in the case where one Entity CA certifies another CA within that Entity for a particular level of assurance that has been mapped to an FBCA certificate level of assurance, the certifying CA must impose CP and CPS requirements (and any other Supplemental Requirements) on the certified CA which are at least as restrictive as the Entity Principal CA's CP and Supplemental Requirements upon which the Federal PKI Policy Authority relied in its policy mapping.

V. Certificate Policy Mapping

A. The mapping of the Entity's certificate levels of assurance (in terms of the FBCA's certificate levels of assurance) shall be as detailed in the table below. This information shall be expressed in the policyMappings extension of the certificate issued by the FBCA to the Entity Principal CA.

FBCA LOA, OID	Entity LOA, OID
Rudimentary	
Basic	
Medium	
High	
Test	

B. The policy mapping shown in the following table shall be expressed in the certificate issued by the Entity to the FBCA.

Entity LOA, OID	FBCA LOA, OID
	Rudimentary
	Basic
	Medium
	High
	Test

C. Unless specifically approved by the Federal PKI Policy Authority, the Entity shall not assert the FBCA CP OIDs in any certificates the Entity CA issues, except in the policyMappings extension establishing an equivalency between an FBCA OID and an OID in the Entity CA's CP.

VI. Dispute Resolution

A. Settlement. Any dispute arising under this Agreement shall be resolved by the Parties. Finally, either Party may terminate this Agreement as set forth below.

[Note. In an MOA with the Government of another Nation, this section may be modified in accordance with the governing law.]

B. Governing Law. The construction validity, performance and effect of this Agreement for all purposes shall be governed by United States Federal law (statute, case law or regulation).

[Note. In an MOA with the Government of another Nation, replace the sentence above with a citation to the treaty or other document under whose authority this MOA is made.]

VII. Liability

Each Party to this agreement shall hold the other harmless with respect to any liability arising out of the operation of the FBCA or the Entity PKI. This agreement is entered into for the convenience of the Parties and shall not give rise to any cause of action by the Parties hereto or by any third party.

VIII. Special Considerations

Special considerations and provisions of this MOA are affixed as Appendix A, "Special Considerations and Provisions." This includes Supplemental Requirements (as defined in Section II), if any.

IX. Termination of the MOA

A. This MOA may be terminated under four circumstances:

1. At the discretion of the Federal PKI Policy Authority. Should the Entity not comply with its obligations under the FBCA CP, Entity CP, CPS, Supplemental Requirements or this MOA, or should an Entity PKI compliance audit indicate unresolved violations of its CP, CPS or Supplemental Requirements, the Federal PKI Policy Authority will evaluate the severity of the noncompliance, and then this MOA and the certificate issued by the FBCA to the Entity may be revoked at the sole discretion of the Federal PKI Policy Authority, upon written notification being provided to the Entity and in accordance with procedures published by the Federal PKI Policy Authority.

2. At the request of the Entity. The certificate issued by the FBCA to the Entity Principal CA may be revoked upon an authenticated request to the FBCA Program Manager or the Chair of the Federal PKI Policy Authority, by a designated official of the Entity responsible for the Principal CA. This official is _____ (see contact information at the end of this MOA).

3. At the discretion of the FBCA Operational Authority. When the FBCA Operational Authority determines that an emergency has occurred that may impact the integrity of the certificates issued by the FBCA, it may immediately revoke a certificate upon authorization of the Chair of the Federal PKI Policy Authority, Chair of the Federal PKI Steering Committee, or other individuals designated by the Federal PKI Policy Authority.

4. At the discretion of the Entity. The Entity, at its sole discretion, may revoke the certificate issued by the Entity to the FBCA. The Entity shall then promptly notify the FBCA Program Manager or the Chair of the Federal PKI Policy Authority, or other individuals designated by the Federal PKI Policy

Authority, in a signed message from the official of the Entity designated in paragraph 2 above.

B. Termination of this MOA will result in the revocation of all cross certificates associated with it.

X. Termination of CA Operation

A. In the event that the Federal PKI Policy Authority decides to terminate the operation of the FBCA, certificates signed by the FBCA shall be revoked, and prior to termination the Federal PKI Policy Authority shall advise entities who have entered into MOAs with the Federal PKI Policy Authority that FBCA operation has terminated so they may revoke certificates they have issued to the FBCA.

B. In the event that the Entity decides to terminate the operation of the Principal CA, the Entity shall advise the Federal PKI Policy Authority prior to termination, and certificates issued by the Principal CA to the FBCA shall be revoked.

XI. Date of Effect

This MOA shall enter into effect upon the signatures of both Parties.

Appendix A
Special Considerations and Provisions

Supplemental Requirements (see II.B, above)
[If none, say so.]

Other
[If none, say so.]

THE PARTIES

FOR THE Federal PKI Policy Authority:

_____
Michelle Moldenhauer
Chair, Federal PKI Policy Authority
Phone 1:
Phone 2:
Email:

Date: _____

FOR THE ENTITY:

_____
XXX
XXXX
Phone 1:
Phone 2
Email:

Date: _____

ACKNOWLEDGED
FOR THE FBCA Operational Authority:

_____
Cheryl Jenkins
FBCA Program Manager
Phone 1:
Phone 2:
Email:

Date: _____

OTHER POINTS OF CONTACT:

ALTERNATE
for the Federal PKI Policy Authority:

XXX
Phone 1:
Phone 2:
Email:

ALTERNATE
for the ENTITY:

XXX
Phone 1:
Phone 2
Email:

CONTACT FOR THE
Entity Operational Authority:

XXX
XXXX
Phone 1:
Phone 2

Email:

ALTERNATE
for the FBCA Operational Authority:

XXX
XXXX
Phone 1:
Phone 2:
Email:

ALTERNATE
for XXXX

XXX
XXXX
Phone 1:
Phone 2
Email:

RECORD OF CHANGES

[to be inserted here or at the front of the document]